

exemption and new Date/Event for automatic declassification based upon the content of previously unreviewed equities.

(c) *Unmarked or improperly marked documents.* Agencies that find other agency information in unmarked or improperly marked documents may apply a different exemption and new Date/Event for automatic declassification based upon the content of previously unreviewed equities.

(d) *Means of Referral.* The reviewing agency must communicate referrals to equity agencies. They may use either of the methods below:

(1) Full text referral. Agencies will make referrals in a format mutually agreed to by the referring and receiving agencies. Each referral request will clearly identify the referring agency and may identify the sections or areas of the document containing the receiving agency's equities and the requested action; or

(2) Tab and notify.

(i) Agencies will use NARA-approved tabs and will clearly indicate on them the agency or agencies having equity in the document(s) held within the tabs. Successive documents with identical equity(ies) may be grouped within a single tab. Documents with differing equities, or non-successive documents, must be tabbed individually. In general, document order may not be changed to facilitate tabbing. In cases where there are so many tabbed documents in a box that tabbing documents individually would seriously overfill the box, the reviewer may group documents under a single tab for each agency equity at the back of each file folder, or back of the box if there is no file folder. If this becomes necessary, the reviewer shall prepare a folder/document list or consult with NARA so that original order can be restored during archival processing.

(ii) Agency notification must include, at a minimum, the following information: the approximate volume of equity, the highest classification of documents, the exact location (to box level) of the documents so marked, and instructions related to access to the boxes containing the documents.

(iii) Agencies will acknowledge receipt of referral notifications. They

should notify the agency that placed the tabs that the review is complete. Any additional equities noted in the review must be annotated on the tab and brought to the attention of the agency that tabbed the document so the tabbing agency can notify those newly identified agencies.

(iv) Equity Notification Database. Agencies may also use an electronic notification database as a means of notification. Use of such a database, when available, will constitute referral and acknowledgement of referrals received under the Order.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for NATO and other foreign government information, agency heads or their designee(s) (hereinafter referred to as agency heads) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director, Information Security Oversight Office (ISOO), to facilitate that office's oversight responsibility. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasure benefits versus cost.

(c) NATO classified information shall be safeguarded in compliance with U.S.

§ 2001.41

Security Authority for NATO Instructions I-69 and I-70. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at §2001.53 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) An agency head who originates or handles classified information shall refer any matter pertaining to the implementation of this Directive that he or she cannot resolve to the Director, ISOO for resolution.

§ 2001.41 Responsibilities of holders [4.1].

Authorized persons who have access to classified information are responsible for:

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

§ 2001.42 Standards for security equipment [4.1].

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment

32 CFR Ch. XX (7-1-08 Edition)

is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

§ 2001.43 Storage [4.1].

(a) *General.* Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) *Requirements for physical protection.* (1) Top Secret. Top Secret information shall be stored by one of the following methods:

(i) In a GSA-approved security container with one of the following supplemental controls:

(A) Continuous protection by cleared guard or duty personnel;

(B) Inspection of the security container every two hours by cleared guard or duty personnel;

(C) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation [Acceptability of Intrusion Detection Equipment (IDE): All IDE must be UL-listed (or equivalent as defined by the agency head) and approved by the agency head. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head.]; or

(D) Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

(ii) An open storage area constructed in accordance with §2001.43, which is equipped with an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not.